

LISTING OF THE CLAIMS:

This listing of claims replaces all prior versions, and listings, of claims in the application:

1-27.

1 28: (Currently Amended) An encoding apparatus comprising:
2 a block cipher key section to be initialized with a block cipher key, having transformation
3 units to transform the block cipher key **(a transformed block cipher key)**;
4 a data section coupled with the block cipher key section to be initialized with a random
5 number, having transformation units to transform the random number based on the transformed
6 block cipher key;
7 a stream cipher key section coupled with the block cipher key section to modify the block
8 cipher key according to a stream cipher key to produce data bits to dynamically modify the
9 random number **(a modified random number)** in the data block section; and
10 a mapping section to receive the modified random number and the transformed block
11 cipher key and generate a pseudo random bit sequence based on the modified random number
12 and the transformed block cipher key.

1 29: (Previously Presented) An apparatus according to claim 28, wherein the block cipher key
2 section further includes first, second, and third registers, to be collectively initialized with the
3 block cipher key.

1 30: (Previously Presented) An apparatus according to claim 29, wherein the block cipher key
2 section further includes substitution units coupled between an output of the first register and an

3 input of the third register, to make at least a partial substitution to the content of the first register
4 and store the substituted content in the third register.

1 31: (Currently Amended) An apparatus according to claim 29, wherein the block cipher key
2 section further includes a linear transformation unit coupled between an output of the second
3 register and an input of the first register and an output of the third register and an input of the
4 second register, to produce a linearly transformed version of the content of the second and third
5 registers, and store the linearly transformed versions in the first and second registers,
6 respectively.

1 32: (Previously Presented) An apparatus according to claim 28, wherein the data section is
2 initialized with plain text.

1 33: (Previously Presented) An apparatus according to claim 28, wherein the data section is
2 initialized with derived random number M_{i-1} .

1 34: (Previously Presented) An apparatus according to claim 28, wherein the data section further
2 includes fourth, fifth, and sixth registers, to be collectively initialized with the random number.

1 35: (Previously Presented) An apparatus according to claim 34, wherein the data section further
2 includes substitution units coupled between an output of the fourth register and an input of the
3 sixth register, to make at least a partial substitution to the content of the fourth register and store
4 the substituted content in the sixth register.

1 36: (Currently Amended) An apparatus according to claim 34, wherein the data section further
2 includes a linear transformation unit coupled between an output of the fifth register and an input
3 of the fourth register and an output of the sixth register and an input of the fifth register, to
4 produce a linearly transformed version of the content of the fifth and sixth registers, and store the
5 **linearly** transformed versions in the fourth and fifth registers, respectively.

1 37: (Previously Presented) An apparatus according to claim 34, wherein the block cipher key
2 section includes first, second, and third registers to be collectively initialized with the block
3 cipher key, and wherein the mapping section comprises a plurality of logical gates coupled with
4 a register in the block cipher key section and a register in the data section.

1 38: (Currently Amended) An apparatus according to claim 28, wherein the stream cipher key
2 section further includes linear feedback **shift** registers (LFSRs) to generate a first, second, and
3 third sequence of data bits, and a serial network of shuffle units to shuffle the third sequence of
4 data bits using the first sequence of data bits **and** input bits and the second sequence of data bits
5 and control bits to the serial network of shuffle units.

1 39: (Currently Amended) An apparatus comprising:
2 a first key section to be enabled in a stream cipher mode and disabled in a block cipher
3 mode, and to selectively modify a cipher key **(a selectively modified cipher key)**;
4 a second key section to be coupled with the first key section in the stream cipher mode,
5 and having a first, second, and third registers to be collectively initialized with the cipher key,

6 and transformation units coupled with the first, second, and third registers to recursively
7 transform the selectively modified cipher key **(a transformed selectively modified cipher key)**;
8 a data section coupled with the second key section, having a fourth, fifth, and sixth
9 registers to be collectively initialized with a data bit sequence, and transformation units coupled
10 with the fourth, fifth, and sixth registers to transform the data bit sequence **(a transformed data**
11 **bit sequence)** according to the transformed selectively modified cipher key; and
12 a mapping section coupled with the second key section and the data section to generate a
13 pseudo random bit sequence with the transformed data bit sequence.

1 40: (Currently Amended) An apparatus according to claim 39, wherein the first key section
2 further includes linear feedback **shift** registers (LFSRs) to generate a first, second, and third
3 sequence of data bits, and a serial network of shuffle units to shuffle the third sequence of data
4 bits using the first sequence of data bits **and** input bits and the second sequence of data bits and
5 control bits to the serial network of shuffle units.

1 41: (Previously Presented) An apparatus according to claim 39, wherein the second key section
2 further includes substitution units coupled between an output of the first register and an input of
3 the third register, to make at least a partial substitution to the content of the first register and
4 store the substituted content in the third register.

1 42: (Currently Amended) An apparatus according to claim 39, wherein the second key section
2 further includes a linear transformation unit coupled between an output of the second register and
3 an input of the first register and an output of the third register and an input of the second register,

4 to produce a linearly transformed version of the content of the second and third registers, and
5 store the linearly transformed versions in the first and second registers, respectively.

1 43: (Previously Presented) An apparatus according to claim 39, wherein the data section is
2 initialized with plain text.

1 44: (Previously Presented) An apparatus according to claim 39, wherein the data section is
2 initialized with derived random number $Mi-1$.

1 45: (Previously Presented) An apparatus according to claim 39, wherein the data section further
2 includes substitution units coupled between an output of the fourth register and an input of the
3 sixth register, to make at least a partial substitution to the content of the fourth register and store
4 the substituted content in the sixth register.

1 46: (Currently Amended) An apparatus according to claim 39, wherein the data section further
2 includes a linear transformation unit coupled between an output of the fifth register and an input
3 of the fourth register and an output of the sixth register and an input of the fifth register, to
4 produce a linearly transformed version of the content of the fifth and sixth registers, and store the
5 linearly transformed versions in the fourth and fifth registers, respectively.

1 47: (Previously Presented) An apparatus according to claim 39, wherein the mapping section
2 comprises a plurality of logical gates coupled with a register in the second key section and a
3 register in the data section.